REMARKS

This response is submitted in reply to the Office Action dated September 22, 2005. Claims 13 – 23 were rejected under 35 U.S.C. 112 and claims 1 – 23 were rejected under 35 U.S.C. 103. In response, Applicants have amended claims 1, 5, 13, 14, 21, 22 and 23 to clarify the claim language and to advance the prosecution of this Application. No new matter has been introduced as a result of the amendments. Applicants respectfully traverses the rejections. Favorable reconsideration is requested.

Claims 13, 14, 21, 22 and 23 and the intervening claims were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description. Applicants respectfully disagree with such, but in an effort to further the prosecution of the application to fully cooperate with the Patent Office, Applicants have amended such claims to eliminate the claim language that allegedly fails to comply with 35 U.S.C. 112, first paragraph. Accordingly, Applicants respectfully submit that the rejection of claims 13, 14, 21, 22 and 23 and the intervening claims is now moot and therefore respectfully request that such rejection be withdrawn.

Claims 1-23 were rejected as being unpatentable over U.S. Patent No. 6,694,436 to Audebert ("Audebert"). Applicants respectfully traverse this rejection, as the cited reference fails to disclose or suggest the features claimed in the present invention. Favorable reconsideration is respectfully requested.

Of the claims pending, claims 1, 5, 13, 14, 21, 22 and 23 are the sole independent claims. Claim 1 is directed to a user authentication system, including: a data holding medium for holding a common key unique to a user, used in a common-key encryption method for authentication between the data holding medium held by the user and an authentication apparatus, and a private key used in a public-key encryption method to the authentication between the data holding medium and a server to perform a service to the user; said authentication apparatus for holding the common key used in the common-key encryption method and a private key used in a public-key encryption method, each unique to the user; and an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method; wherein the authentication apparatus performs authentication, authenticating the data holding medium by using the common key used in common-key encryption method for the user held by the data

holding medium, in response to an authentication request sent from the information processing apparatus, and, only when the user has been authenticated, performs processing for making the information processing apparatus authenticate the user by using the private key corresponding to the user, wherein information encrypted by the public-key encryption method is sent from the information processing apparatus, forwarded to the authentication apparatus, decrypted using the private key corresponding to the user so as to obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 5 is directed to a user authentication method for a user who carries a data holding apparatus for holding a common key unique to a user, used in a common-key encryption method for authentication of the data holding apparatus held by the user and an authentication apparatus for authentication between the data holding apparatus and a server to perform a service to the user, the method including the steps of: authenticating the data holding apparatus of the user by the common-key encryption method by using the common key held by the data holding apparatus in response to an authentication request from the server; and performing, only when the user has been authenticated, processing for authenticating the user by a public-key encryption method.

Claim 13 is directed to an authentication method, including the steps of: holding a common key unique to a user used in a common-key encryption method for authentication between a data holding apparatus held by the user and an authentication apparatus, and a private key used in a public-key encryption method to the authentication between the data holding apparatus and a server to perform a service to the user; authenticating, in response to an authentication request sent from an external information processing apparatus, the data holding apparatus by using the held common key used in the common-key encryption method for the user held by the data holding apparatus; and performing, only when the data holding apparatus has been authenticated in the authentication step, processing for making the information processing apparatus authenticate the data holding apparatus by the public-key encryption method by using the private key corresponding to the user, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, decrypted by an authentication device using the private key corresponding to the user so as to

obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding apparatus.

Claim 14 is directed to an authentication apparatus, including: a holder for holding a common key unique to a user, used in a common-key encryption method for authentication between a data holding medium held by the user and an authentication apparatus, and a private key used in a public-key encryption method to the authentication between the data holding medium and a server to perform a service to the user; an authenticating device for, in response